1. (Currently amended) A method of providing secure transmissions from a biometric smartcard reader, said method comprising the steps of:

encrypting a signal created by said biometric smartcard reader dependent on ~~said~~ a smartcard containing biometric data, said smartcard reader able to obtain biometric data directly, said signal comprising access information dependent upon biometric data obtained directly by said biometric smartcard reader from a user and said biometric data contained in said smartcard;

transmitting said encrypted signal to a high security module at a remote location relative to said biometric smartcard reader;

translating by said high security module at said remote location said transmitted signal to another format useable by an access controller; and

controlling an access mechanism using said access controller dependent upon said translated signal.

2. (Cancelled)

3. (Currently amended) The method according to claim ~~2~~ 1, wherein said biometric data comprises fingerprint data.

4. (Currently amended) The method according to claim ~~2~~ 1 wherein said biometric data is not transmitted to said high security module at said remote location from said smartcard reader.

5. (Previously presented) The method according to claim 1, further comprising the step of providing access using said access mechanism if said translated signal is determined by said access controller to authorize access.

6. (Original) The method according to claim 5, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

7. (Previously presented) The method according to claim 1 wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

8. (Previously presented) The method according to claim 1 wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

9. (Currently amended) The method according to claim 1, further comprising the step of encrypting communications between said biometric smartcard and said biometric smartcard reader.

10. (Cancelled)

11. (Currently amended) The method according to claim ~~10~~ 9, wherein said high security module translates said encrypted signal to said other format.

12. (Currently amended) The method according to claim ~~10~~ 9, wherein said biometric smartcard reader and said high security module are separated by a distance of up to 1.2 kilometers.

13. (Currently amended) The method according to claim ~~10~~ 9, wherein said biometric smartcard reader and said high security module are separated by a distance of up to 15 meters.

14. (Previously presented) The method according to claim 1 wherein said translated signal is in a controller-specified format.

15. (Original) The method according to claim 14, wherein said controller-specified format is Wiegand format, or clock and data.

16. (Currently amended) A system for providing secure transmissions from a biometric smartcard reader, said system comprising:

a biometric smartcard reader for encrypting a signal created by said biometric smartcard reader dependent on said smartcard containing biometric data, said smartcard reader able to obtain biometric data directly, said signal comprising access information dependent upon biometric data obtained directly by said biometric smartcard reader from a user and said biometric data contained in said smartcard, and for transmitting said encrypted signal using a communications protocol to a remote location relative to said biometric smartcard reader;

a high security module for receiving said transmitted signal and translating said transmitted signal to another format useable by an access controller; and

an access controller for controlling an access mechanism using said access controller dependent upon said translated signal.

17. (Cancelled)

18. (Currently amended) The system according to claim ~~17~~ 16, wherein said biometric data comprise fingerprint data.

19. (Currently amended) The system according to claim ~~17~~ 16 wherein said biometric data is not transmitted to said high security module from said biometric smartcard reader.

20. (Previously presented) The system according to claim 16, further comprising an access mechanism providing access if said translated signal is

determined by said access controller to authorize access.

21. (Original) The system according to claim 20, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

22. (Previously presented) The system according to claim 16 wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

23. (Previously presented) The system according to claim 16 wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

24. (Currently amended) The system according to claim 16, wherein communications between said biometric smartcard and said biometric smartcard reader are encrypted.

25. (Currently amended) The system according to claim 24, wherein said biometric smartcard reader and said high security module are separated by a distance of up to 1.2 kilometers.

26. (Currently amended) The system according to claim 24, wherein said biometric smartcard reader and said high security module are separated by a distance of up to 15 meters.

27. (Previously presented) The system according to claim 16 wherein said translated signal is in a controller-specified format.

28. (Original) The system according to claim 27, wherein said controller-specified format is Wiegand format, or clock and data.

29-31. (Cancelled)

32. (New) The system as claimed in claim 16 wherein said encrypted signal is transmitted using a communications protocol and said high security module decrypts said transmitted signal, said communications protocol being different from said format useable by said access controller.

33. (New) The system as claimed in claim 32 wherein said transmitted signal is transmitted using one of RS-232 and RS-485 communications protocol.